

Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method for secure authentication of a user in a session conducted over a two-way telephony communication channel, comprising:

allowing the user to access an authenticating entity via a two-way telephony communication channel;

inserting a session identifier by the authenticating entity into the two-way telephony communication channel that is infeasible to detect or eliminate without knowledge of a secret known to the authenticating entity, wherein inserting the session identifier into the communication channel further comprises inserting pseudorandom noise deterministically generated according to the secret known only to the authenticating entity into the communication channel by the authenticating entity;

receiving authentication information for the user by the authenticating entity via the two-way telephony communication channel;

analyzing the authentication information by the authenticating entity to determine whether the session identifier inserted by the authenticating entity into the two-way telephony communication channel is associated with the received authentication information; and

authenticating the user by the authenticating entity based on the authentication information if the session identifier is found to be associated with the authentication information.

2. (Original) The method of claim 1, wherein the user further comprises one of a voice user and a touch tone keypad user.
3. (Original) The method of claim 1, wherein the authenticating entity further comprises a financial institution.
4. (Original) The method of claim 1, wherein the two-way telephony communication channel further comprises one of a two-way land line telephony communication channel, a two-way wireless telephony communication channel and a two-way voice over Internet protocol (VoIP) telephony communication channel.
5. (Original) The method of claim 1, wherein the two-way telephony communication channel further comprises one of a two-way hard-wired telephony communication channel, a two-way satellite telephony communication channel, and a two-way microwave telephony communication channel.
6. (Canceled)
7. (Currently amended) The method of claim 6 1, wherein the secret known only to the authenticating entity further comprises a pre-determined seed in combination with a pre-selected algorithm for generating the pseudorandom noise.
8. (Original) The method of claim 7, wherein inserting the session identifier into the two-way telephony communication channel further comprises injecting a session identifier modulated by the pseudorandom noise into the communication channel by the authenticating entity.
9. (Original) The method of claim 1, wherein inserting the session identifier into the communication channel further comprises inserting the session identifier into the two-way telephony communication channel by the authenticating entity during an initial personal identification number (PIN) training session for the user.

10. (Original) The method of claim 1, wherein inserting the session identifier into the communication channel further comprises inserting a different session identifier into the communication channel by the authenticating entity during each session in which authentication information consisting at least in part of a personal identification number (PIN) is entered for the user.

11. (Original) The method of claim 1, wherein receiving the authentication information further comprises receiving authentication information for the user that is entered at least in part by speaking the authentication information.

12. (Original) The method of claim 1, wherein receiving the authentication information further comprises receiving authentication information for the user that is entered at least in part on a touch tone keypad.

13. (Original) The method of claim 1, wherein the authentication information consists at least in part of a personal identification number (PIN) for the user that is entered by one of speaking the PIN and a touch tone keypad..

14. (Currently amended) The method of claim 6 1, wherein analyzing the authentication information further comprises analyzing pseudorandom noise associated with the authentication information by the authenticating entity to determine whether it is the same as the pseudorandom noise inserted by the authenticating entity into the communication channel.

15. (Original) The method of claim 7, wherein analyzing the pseudorandom noise further comprises analyzing the pseudorandom noise associated with the authentication information using the pre-determined seed in combination with the pre-selected algorithm.

16. (Original) The method of claim 1, wherein analyzing the authentication information further comprises identifying a playback of a recording of a session

identifier inserted by the authenticating entity into the two-way telephony communication channel on a preceding occasion.

17. (Currently amended) A system for secure authentication of a user in a session conducted over a two-way telephony communication channel, comprising:

means for allowing the user to access an authenticating entity via a two-way telephony communication channel;

means for inserting a session identifier by the authenticating entity into the two-way telephony communication channel that is infeasible to detect or eliminate without knowledge of a secret known to the authenticating entity, wherein the means for inserting the session identifier into the communication channel further comprises a pseudorandom noise generator adapted for inserting a pseudorandom noise deterministically generated according to the secret known only to the authenticating entity into the communication channel by the authenticating entity;

means for receiving authentication information for the user by the authenticating entity via the two-way telephony communication channel;

means for analyzing the authentication information by the authenticating entity to determine whether the session identifier inserted by the authenticating entity into the two-way telephony communication channel is associated with the received authentication information; and

means for authenticating the user by the authenticating entity based on the authentication information if the session identifier is found to be associated with the authentication information.

18. (Original) The system of claim 17, wherein the user further comprises one of a voice user and a touch tone keypad user.

19. (Original) The system of claim 17, wherein the authenticating entity further comprises a financial institution.
20. (Original) The system of claim 17, wherein the two-way telephony communication channel further comprises one of a two-way land line telephony communication channel, a two-way wireless telephony communication channel and a two-way voice over Internet protocol (VoIP) telephony communication channel.
21. (Original) The system of claim 17, wherein the two-way telephony communication channel further comprises one of a two-way hard-wired communication channel, a two-way satellite communication channel, and a two-way microwave communication channel.
22. (Canceled).
23. (Currently amended) The system of claim 22 17, wherein the secret known only to the authenticating entity further comprises a pre-determined seed in combination with a pre-selected algorithm for generating the pseudorandom number.
24. (Original) The system of claim 23, wherein the means for inserting the session identifier into the two-way telephony communication channel further comprises a pseudorandom noise generator adapted for injecting a session identifier modulated by the pseudorandom noise into the communication channel.
25. (Original) The system of claim 17, wherein the means for inserting the session identifier into the communication channel further comprises means for inserting the session identifier into the two-way telephony communication channel by the authenticating entity during an initial personal identification number (PIN) training session for the user.
26. (Original) The system of claim 17, wherein the means for inserting the session identifier into the communication channel further comprises means for

inserting a different session identifier into the communication channel by the authenticating entity during each session in which a PIN is entered for the user.

27. (Original) The system of claim 17, wherein the means for receiving the authentication information further comprises means for receiving authentication information for the user that is entered at least in part by speaking the authentication information.

28. (Original) The system of claim 17, wherein the means for receiving the authentication information further comprises means for receiving authentication information for the user that is entered at least in part on a touch tone keypad.

29. (Original) The system of claim 17, wherein the means for receiving the authentication information consists at least in part of a personal identification number (PIN) for the user that is entered by one of speaking the PIN and a touch tone keypad..

30. (Currently amended) The system of claim ~~22~~ 17, wherein the means for analyzing the authentication information further comprises means for analyzing pseudorandom noise associated with the authentication information by the authenticating entity to determine whether it is the same as the pseudorandom noise inserted by the authenticating entity into the communication channel.

31. (Original) The system of claim 23, wherein the means for analyzing the pseudorandom noise further comprises means for analyzing the pseudorandom noise associated with the authentication information using the pre-determined seed in combination with the pre-selected algorithm.

32. (Original) The system of claim 17, wherein the means for analyzing the authentication information further comprises means for identifying a playback of a recording of a session identifier inserted by the authenticating entity into the two-way telephony communication channel on a preceding occasion.